



BEST BEST & KRIEGER
ATTORNEYS AT LAW

www.BBKlaw.com

INDIAN WELLS
IRVINE
LOS ANGELES
MANHATTAN BEACH
ONTARIO
RIVERSIDE
SACRAMENTO
SAN DIEGO
WALNUT CREEK
WASHINGTON, D.C.

REPORT TO THE CITY OF LONG BEACH

LONG BEACH POLICE DEPARTMENT ACQUISITION & USE OF THE TIGERCONNECT INSTANT MESSAGING APP LEGAL & POLICY ISSUES

December 2018

Gary W. Schons
Of Counsel
Best Best & Kriger LLP

Indian Wells
(760) 568-2611

Irvine
(949) 263-2600

Los Angeles
(213) 617-8100

Manhattan Beach
(310) 643-8448

Gary W. Schons
(619) 525-1348
gary.schons@bbklaw.com
File No. 65192.00010



BEST BEST & KRIEGER
ATTORNEYS AT LAW

655 West Broadway, 15th Floor, San Diego, CA 92101
Phone: (619) 525-1300 | Fax: (619) 233-6118 | www.bbklaw.com

Ontario
(909) 989-8584

Riverside
(951) 686-1450

Sacramento
(916) 325-4000

Walnut Creek
(925) 977-3300

Washington, DC
(202) 785-0600

November 30, 2018

Patrick H. West, City Manager
City of Long Beach

Charles Parkin, Esq., City Attorney
City of Long Beach

Re: TigerConnect

Dear Messrs. West and Parkin:

This firm and its attorneys are dedicated to assisting its public entity clients in achieving and maintaining governance marked by transparency, probity and integrity in compliance with the law, sound policy and “best practices.” We are honored to have been selected by the City of Long Beach and privileged to be commissioned to conduct this review and provide this report. We hope that this report will assist the City in moving forward, not only with respect to the use of the TigerConnect app by the Police Department, but with other challenges posed at the intersection of law, policy and technology.

This review and report benefitted from the cooperation and professionalism of the City Manager’s Office, the City Attorney and his office, particularly Assistant City Attorney Michael Mais and Deputy City Attorney Monica Kilaita, the Police Department under the direction of Chief Robert Luna and with the assistance of Commander Erik Herzog, and the professionals in the City’s Technology and Innovation Department.

While the work for which we were commissioned is completed with the provision of this report, we would welcome the opportunity to assist the City in explaining its findings, conclusions and recommendations to your policy makers and public, as appropriate, and in achieving whatever goals the City might set out for moving forward.

Sincerely,

A handwritten signature in blue ink that reads 'Gary W. Schons'.

Gary W. Schons
Of Counsel for
for BEST BEST & KRIEGER LLP

TABLE OF CONTENTS

	Page
INTRODUCTION.....	1
Background.....	1
Purpose of Review and Report	1
Qualifications of the Reviewer.....	2
Sources and Methods.....	2
Analytical Construct	4
Structure of the Report.....	4
Executive Summary of Findings.....	4
TIGERCONNECT.....	7
What Is TigerConnect?	7
How Does the TigerConnect App Operate?	7
What Is a “Message Lifespan”?	8
“Ephemeral” or Self-Destructing Messaging Apps	8
LONG BEACH POLICE DEPARTMENT’S ACQUISITION, DEPLOYMENT AND USE OF THE TIGERCONNECT APP	10
Acquisition of the TigerConnect App	10
Deployment of the TigerConnect App	12
Use of the TigerConnect App.....	12
No Evidence Supports Claims of Illegal Use or Misuse of TigerConnect, No Complaints or Reports of Adverse Effects in Criminal or Civil Cases	13
LEGAL AND POLICY IMPLICATIONS FOR THE USE OF TIGER CONNECT BY THE PD.....	15
Compliance with City and Departmental Policies.....	15
Compliance with the Public Records Act (Gov’t Code § 6250 et seq.)	19
Compliance with Constitutional and Statutory Evidence Retention and Disclosure Obligations in Criminal Prosecutions	20
Compliance with Civil Litigation Evidence Retention & Discovery Requirements (“spoliation of evidence”)	23
“BEST PRACTICES” FOR THE USE OF TIGER CONNECT OR OTHER EPHEMERAL MESSAGING APPS BY THE PD AND THE CITY.....	24
ENDNOTES	28
APPENDIX A	

INTRODUCTION

Background

In a September 18, 2018, article, *Al Jazeera* reported that the Long Beach Police Department (“PD”) “may have used [TigerConnect] to share sensitive and potentially incriminating information that they wouldn’t want to be disclosed to a court.” The article went on to report that “[two] police officers who spoke with *Al Jazeera*...claimed they were instructed by their superiors to use the app to ‘have conversations with other officers that wouldn’t be discoverable.’ They said they understood this to include exculpatory evidence that could be potentially helpful to attorneys in both civil and criminal proceedings against the department.” The article went on to report that “[i]n response to *Al Jazeera*’s investigation, PD said it ‘complies with all laws related to discovery, and any information relevant to a specific investigation would be documented and provided according to legal requirements.’”

Later that same day the City Manager issued a response to the media announcing that the use of TigerConnect had been suspended by order of the Chief of Police¹ pending review which would encompass “[a]s part of the review of internal communication practices, the city will be reviewing best practices, current case law, and city policies.” The City also created a website as a repository for information available to the public and documents related to the TigerConnect matter.² This made all Public Records Act requests and disclosures available to the public.

Purpose of Review and Report

On September 21, the City announced that it would obtain “an independent outside review of the Long Beach Police Department’s use of a direct messaging application called Tiger Connect. The review was initiated by the City Manager in partnership with the City Attorney and will consist of an outside firm hired to independently review the use of the messaging application within the Long Beach Police Department.”³ As announced, “[t]he review will include, but not be limited to:

- The origin and implementation of the messaging application within the Police Department and the Technology and Innovation Department.
- City policies and procedures related to mobile messaging.
- How the messaging app was utilized.
- Policies and procedures for documentation of evidence.
- The City’s record retention policies.
- Best practices for other law enforcement entities related to messaging applications.
- State law and any other relevant topics.

“The outside review will be done in conjunction with the City Attorney’s Office, and the results will be made available to the public to the extent allowable under California State law.”⁴

Within a week, this firm was approached and then engaged to conduct this review and provide a report.

Qualifications of the Reviewer

The review was conducted and report composed by Gary W. Schons, Esq., Of Counsel to the firm of Best, Best Best & Krieger LLP, where he is head of the firm’s Public Policy and Ethics Compliance Group. Prior to joining Best Best & Krieger, Mr. Schons served for 35 years in the Criminal Division of the California Attorney General’s Office, including assignments to the Appeals, Writs & Trials Section, Special Prosecutions Unit, Asset Forfeiture Program, and various local, state and federal task forces. From 1991 until 2011, Mr. Schons headed the Criminal Division of the Attorney’s General Office in San Diego, where he supervised some 74 Deputy Attorneys General who handled over 2,000 felony criminal appeals annually, in excess of 200 death penalty cases, and numerous public corruption and official misconduct investigations and prosecutions. He has prosecuted felony cases in the state and federal trial courts, and briefed and argued cases in nearly all of the state’s appellate courts, the State Supreme Court, the Ninth Circuit Court of Appeals and the United States Supreme Court. After retiring from state service in 2011, Mr. Schons joined the San Diego County District Attorney’s Office where he served as Senior Advisor for Law & Policy and as a Deputy Attorney District Attorney, advising the District Attorney and that office’s executive staff.

In his career, Mr. Schons has served as Trial Counsel for the Commission on Judicial Performance and as Special Trial Counsel for the California State Bar. He has received numerous awards from statewide and national prosecution organizations, including the California District Attorneys Association’s Career Achievement Award. He is an adjunct professor of Criminal Procedure and Moot Court at the University of San Diego School of Law, where he serves on its Board of Visitors and has been recognized with the school’s Distinguished Alumni Award.

Sources and Methods

The City Attorney’s Office provided a briefing into the background of the TigerConnect issue and collaborated on an investigative plan and report proposal as outlined in a formal memo provided to it setting out project objectives and an investigation plan.

The City Attorney assigned a Deputy City Attorney to act as a liaison with that and other City offices, and the Chief of Police assigned a command level officer to serve as a liaison with the PD. The PD provided an annotated timeline it had prepared internally regarding the origin and history of its use of the TigerConnect app.

All of the City's TigerConnect materials, consisting of scores of documents, were collected and reviewed. These materials documented the acquisition, deployment and use of the TigerConnect app by the PD. On-line and other research was conducted into TigerConnect, the company, the product and product history. Through the PD liaison, TigerConnect provided metadata related to the department's use of the TigerConnect app. Additionally, on-line research was conducted concerning the PD's forerunner instant messaging system---the Blackberry platform. On-line research was conducted into the development and use of various "ephemeral" messaging applications, like TigerConnect, and the emerging and now widespread use of this technology by governments, enterprises and individuals.

All media reports related to the PD's use of the TigerConnect app were collected and reviewed with a focus on identifying alleged claims and issues leveled in connection with that use. Additionally, meetings of the City Council's Public Safety Committee and the City's Citizen Police Complaint Commission were reviewed, as critics of the use of the TigerConnect app by the PD spoke at those meetings and identified their complaints and concerns. An individual, who authored media articles referencing anonymous sources connected to the PD, who had asserted misuse of the TigerConnect app, and who appeared at a Citizen Police Complaint Commission meeting to register such a complaint and seek an investigation, was contacted and requested to provide any evidence, witnesses or sources to corroborate claims of misuse or illegal use of the TigerConnect app by the PD or any of its officers. That individual declined to provide any information or cooperate with this investigation.

All relevant City Charter, Municipal Code and City policy provisions, as well as relevant written policies and procedures of the PD, were collected, reviewed and analyzed. Extensive legal research was conducted into governmental policy formation relevant to the use of this type of technology and data retention, state laws, including records retention statutes and the Public Records Act, state and federal constitutional law affecting the duty to retain and disclose evidence in criminal cases, and laws and statutes related to discovery spoliation in civil cases. The use of the TigerConnect app by the PD was analyzed for compliance with these policies and legal requirements, on their face and in practice.

Command level officers most knowledgeable of the TigerConnect app's acquisition, deployment and use by the PD, including the Chief of Police, were interviewed, as were a number of civilian City employees with assignments to PD IT and the City's Technology and Innovation Department, who had been involved with the acquisition, deployment and management of the app.

Contact was made with the Long Beach City Prosecutor and ranking members of the Los Angeles County District Attorney's Office to determine if the PD's use of the TigerConnect app had affected any criminal prosecutions conducted by those offices.

Finally, research was conducted and legal and policy makers were interviewed to identify "best practices" as applied to the use of the TigerConnect technology.

Analytical Construct

As commissioned by the City Attorney and City Manager, the review sought to create a history of the origin and implementation of the TigerConnect messaging app within the PD and the Technology and Innovation Department. In connection with this aspect of the investigation, the background for acquiring the app, how and why it was acquired, and how it was deployed and utilized by the PD were examined.

The claims made of misuse and illegal use by the PD of the TigerConnect app which prompted this review are set out, analyzed and assessed for their logic and legal implications and for any evidence to support them.

City policies and procedures related to mobile instant messaging, policies and procedures for documentation of evidence and the City's record retention policies were reviewed, analyzed and assessed for compliance in connection with the use of the TigerConnect app by the PD. State and federal law related to records and evidence retention and disclosure were likewise researched, analyzed and assessed within the context of the TigerConnect app as used by the PD. The standard for thorough and complete legal research, judgment and advice expected of legal counsel were applied to these determinations and those were reviewed by a number of this firm's counsel internally.

Finally, research was conducted into "best practices" for policy formation and deployment by government entities related to such messaging applications and technology.

Structure of the Report

This report is divided into four substantive parts. The first section is a discussion of the TigerConnect app, itself, and, the emerging and expanding use of "ephemeral" instant messaging applications in society at large. The second part traces the history of the PD's prior instant messaging technology, the search for, discovery, study and decision to acquire TigerConnect, and then, its deployment and use by the PD. The third section is an analysis of relevant City and PD policies as applied to the use of the TigerConnect app by the PD, and compliance with relevant state and federal laws related to records and evidence retention and disclosure. The final section discusses "best practices" to guide the selection and implementation of this kind of technology, followed by recommendations to ensure the City's appropriate implementation of such "best practices."

Executive Summary of Findings

- TigerConnect is a secure messaging app, now known as an "ephemeral messaging app," which allows users to share encrypted messages that automatically delete after a set period of time

- “Ephemeral messaging” is the mobile-to mobile transmission of messages that automatically disappear from the recipient’s screen after the message has been viewed or a pre-determined time has lapsed (“Message Lifespan”)
- “Ephemeral messaging” has existed for decades---a telephone call
- For over ten years prior to the PD’s acquisition and deployment of the TigerConnect app, PD command staff and officers in certain designated units were assigned Blackberry devices as personal telephones and messaging devices; this platform had a built-in “ephemeral” messaging capability with a message lifespan of 3 days
- In 2013, the City and the PD started to switch over to the Apple iPhone, however, acquisition and deployment of the iPhone was held up by the lack of a secure instant messaging app for the iPhone platform, like that then available on Blackberry
- TigerConnect, which could be used on the iPhone platform, was found to be a secure app able to replace the Blackberry system as accessible to and serve only those in a controlled group assigned the app, secure by end-to-end encryption, not reliant on or connected to the City’s servers, had a message self-destruct or message lifespan capability, provided verification of messages as read, and was capable of sending group messages and to create messages by verbal dictation
- PD acquired TigerConnect in June 2014 with a purchase order approved within PD as within its spending authority and sent for execution by the Technology and Innovation Department; iPhones with the TigerConnect app “pushed” by the Technology and Innovation Department, were deployed to select PD personnel in July or August 2014
- There was no City Manager review or approval of the purchase and deployment because none was required and the City Attorney was not consulted because the technology was viewed as simply replacing the similar Blackberry technology previously in use
- There is no evidence that TigerConnect was acquired other than in conformance with the spending approval and technology acquisition policies of the PD and the City
- TigerConnect provides PD users with a constant and reliable means of transitory, immediate and secure communication
- PD uses the TigerConnect messaging app for notifications within and between members of the assigned group of officers concerning emerging events or incidents, whereabouts, and time and need to respond, “call outs,” operational planning, needs and communication, and status or results of operations in

nearly real time. It has proven to be more flexible, efficient, speedy and effective than a telephone call or in person conversation because of its continuous operation, message prompts and ability to message multiple parties in a single use and produce read receipts and string responses

- PD does not use the TigerConnect app for “note taking” or as a replacement for any aspect of PD official report writing or evidence retention as it is not a note-taking or data storage app or system
- There is no evidence that the PD’s use of TigerConnect has been or is in violation of City or PD regulations or policies
- There is no evidence to support claims of illegal use or misuse of the TigerConnect app by the PD, and no complaints or reports of adverse effects in criminal or civil cases
- The Los Angeles County District Attorney’s Office and Long Beach City Prosecutor advise that there have been no issues created in or of any adverse effects on any criminal matters prosecuted by those offices which were investigated by the PD as a result of the use of the TigerConnect app
- The City Attorney reports there have been no adverse effects in civil cases affecting or involving the City, nor has any litigant or court of record raised a concern over the use of the TigerConnect app by the PD
- No individual has come forward to make or substantiate any of the claims of misuse of illegal use of the TigerConnect app by the PD as reported in the media articles which prompted this review
- It appears that the use of the TigerConnect app by the PD is in compliance with existing and emerging policies of the City concerning records retention, as well as state law on the subject
- The self-destruction of messages on the TigerConnect app, and the policies of the City permitting that function, do not violate or prevent compliance with the Public Records Act
- The use of the TigerConnect app by the PD does not violate constitutional or statutory requirements for the retention and disclosure of evidence in criminal cases and there are no reports of constitutional or statutory discovery issues in cases prosecuted in which the PD was an investigating agency
- The operation of the TigerConnect messaging app would not, outside the context of active litigation, be considered “spoliation,” subject to any type of discovery sanction by the courts, resulting in prejudice to the City in its civil litigation

- The City could now undertake applicable policy review to ensure those measures comprehend this technology, address its uses and are consistent with overall communication policies

TIGERCONNECT

What Is TigerConnect?

TigerConnect⁵ is a messaging app for use on iOS, macOS and Android devices. TigerConnect is a cloud-based communication platform for instant messaging or texting.⁶ The company is based in Los Angeles and was founded in 2010 by Andrew Brooks MD and Brad Brooks as TigerText, with the original goal of increasing clinical medical communication and collaboration in a secure environment, compliant with HIPAA patient privacy requirements. According to reports, in July 2012, the application announced API integration with Dropbox, which allows its users to send secure documents in a secure format. In March 2018, TigerText was rebranded as TigerConnect..

TigerConnect is within the broad category of secure messaging apps now known as “ephemeral messaging apps,” which allows users to share encrypted messages that automatically delete after a set period of time, to remove all traces from a conversation, and to share documents. It is designed to work across large organizations and with multiple connected users.

TigerConnect reports that it has not sold this messaging app to any law enforcement agency other than the PD. It has, however, sold this product to three other government entities.

How Does the TigerConnect App Operate?

As described by the company: “TigerConnect ensures that the right information is instantly accessible at the point of care and helps care teams communicate in real time, on any device, through a suite of messaging features tailor-made for healthcare productivity. TigerConnect’s secure, encrypted HITRUST certified application protects patient information and meets HIPAA guidelines, even guaranteeing your organization against fines. [With TigerConnect, users can:]

- Save time and improve communication efficiency by alleviating phone tag, unanswered pages and disruption to patients and care team members.
- Enable staff to quickly communicate and coordinate with other departments for consults transfers, medication reconciliation, and more.
- Keep messages private with a fully encrypted, end-to-end, secure texting solution.
- Send high priority messages that stay at the top of the recipient’s in box and specify a unique alert for instant differentiation.

- Have messages automatically forwarded to another colleague when in Do Not Disturb Mode.
- Know instantly when messages have been sent, delivered, and read.
- Set message lifespan to dictate when messages will be automatically deleted.
- Recall a message and attachments before or after it has been read.
- Create groups to improve collaboration and see who has read your message and when.
- Securely attach photos, voice notes, PDFs, and other files right from apps like Box, Google Drive, and more.”

“To know whether a message has been read, each message that has been sent will provide notice to the sender with a status on the bottom right corner of the message. When a message has been Read on iOS, the word ‘Read’ will appear in the lower right-hand corner of the message. This assumes that the user has opened the message, and viewed the contents of the message.

“To know if a message sent by another is received a message on iOS, the receiver will receive a ‘push notification’ on the device to advise of receipt of a TigerConnect message. This comes in the form of an audible ringtone and a visual notification.

“To send a message the TigerConnect app allows users to message only with users in the organization that the administrator has added.”

What Is a “Message Lifespan”?

Message lifespan is the length of time a message will remain in a TigerConnect conversation before it is deleted on both the sender’s and all recipients’ devices. This applies to individual conversations as well as group messages. For example, if a message lifespan is 2 days and is sent to another user at 2:00 PM on Friday and received to their device, but it is not opened to mark it as “Read,” until 2:00 PM Sunday, the message is no longer visible to the sender. The message is deleted from the sender’s device, the receiver’s device, and the server, that is, it is no longer in TigerConnect. The message cannot then be forwarded or stored unless TigerConnect has been tasked with archiving messages.

“Ephemeral” or Self-Destructing Messaging Apps

“Ephemeral messaging” is the mobile-to mobile transmission of messages that automatically disappear from the recipient’s screen after the message has been viewed or a pre-determined time has lapsed (“Message Lifespan”). It is an outgrowth of the growing and now ubiquitous use of instant messaging or texting. This technology has

reshaped digital communication at the personal and enterprise levels. The success of Snapchat, started in 2011, has inspired a whole range of “ephemeral” messaging apps for consumers, businesses and government entities concerned about security and privacy.

The technology was viewed as breakthrough as recently as 2013. One scholarly article described the motivation to employ “ephemeral messaging”:

“As Internet-connected smartphones are prevalent nowadays, instant messaging applications on these devices are very popular, resulting in more and more people using mobile messaging apps in their daily communication with their peers. In addition to one-to-one conversations, these apps facilitate group chats and support various message types such as text, picture, video, or voice messages.

“In contrast to face-to-face talks or telephone calls, the course of a conversation in mobile messaging is usually logged by each participant. Logging makes the communication persistent and allows previously uninvolved third parties to retrieve past communication from the message history. Since communication in mobile messengers is often informal, it seems plausible that messages are often of ephemeral nature and not meant to be stored permanently.”⁷

It is reported that many enterprises are deploying and allowing the use of “ephemeral messaging apps” to protect sensitive internal communications in the workplace. Such messaging apps are encrypted and secure from breaches and messages on the systems can be instantly and permanently deleted. Many messages are not stored on servers. It is widely recognized that enterprises greatly reduce the risk of data breach and enhance security if communications are ephemeral, particularly sensitive internal communications.

In addition to Snapchat, these “ephemeral,” self-destructing messaging apps include Frankly, Blink, Wickr,⁸ Telegram, WhatsApp, Perfect Serve, Telemediq, Spok, qlipSoft, Lua and Confide, and offer features such as encrypted messages, disappearing photos and the like. Gmail has recently added “Confidential Mode,” an “ephemeral” app to its platform. As reported, “emails sent using the confidential mode, for instance, are erased after a designated time set by the user. Until they are erased, they are stored directly on Google’s servers instead of on a proprietary company-owned server. And even if a Gmail user sends an email under confidential mode to a recipient who is using a different email client, the recipient can only access that email via a website link that still connects to Google’s servers.”⁹

“Ephemeral messaging” is today in widespread use and here to stay (until eclipsed by more advanced technology). However, as one tech expert has noted, “We’ve had ephemeral messaging for decades---it’s called a phone call.”¹⁰

In addition to TigerConnect, the City has deployed Snapchat which has “ephemeral messaging” capabilities. That app is deployed on nine devices for social

media purposes, which are assigned to users in the offices of City Manager, Development Services, Disaster Preparedness & Emergency Communications, Health & Human Services, Legislative (City Council and staff), and Parks, Recreation & Marine.

LONG BEACH POLICE DEPARTMENT'S ACQUISITION, DEPLOYMENT AND USE OF THE TIGERCONNECT APP

Acquisition of the TigerConnect App

This review found that for over ten years prior to 2013, command staff (rank of Lieutenant and higher in the PD) and sworn personnel in certain designated units---Internal Affairs, Crime Intelligence Section (which includes anti-terrorism assignments) and Homicide---were assigned Blackberry devices as personal telephones and messaging devices. This group, composed of command and sworn officers with "need to know" assignments, included approximately one hundred of the PD's 1,214 employees.

Each Blackberry device was assigned a unique personal identification number (PIN) at time of manufacture, and the devices deployed to this group were supplied with the Blackberry Messenger ("BBM"), which enabled PIN to PIN messaging, including secure single person or group messaging among those assigned the devices, which bypassed the email system. Messages sent using BBM were secure in that they are end-to-end encrypted, and not stored on a server. Messages sent using BBM could be made to self-destruct or include a limited viewing time. Thus, BBM was one of, if not the earliest, "ephemeral messaging app." (The PD's BBM was set to self-delete messages in 3 days.) The Federal Bureau of Investigation, Central Intelligence Agency, Department of Defense and Department of Homeland Security have deployed and used the Blackberry devices with BBM for years, according to reports.

In this review, it was found that at the end of 2013, the PD was advised that it would no longer have access to the Blackberry PIN feature and the ability to use BBM for messaging. At that time, the City and the PD started looking at switching over to the Apple iPhone. However, acquisition and deployment of the iPhone was held up by the lack of secure instant messaging app available on the iPhone platform at the time to the assigned group of command and sworn officers. Such secure messaging technology was vital to this group in the PD because of the sensitive information often included in these instant messages which could relate to violent crimes, security and emergency matters, crime victims, confidential sources of information, operational plans, and personnel matters, among others. Such messages could not be stored on the City's servers because they could then be accessed by non-sworn personnel and sensitive information could be compromised or misused.

Commander (then Lt.) Lloyd Cox, who had prior assignments going back years in the PD's technology unit ("PD IT"), was tasked with exploring technology solutions for sworn officers for the PD, including secure messaging for the iPhone. He had discussed the need for such an application with Scott Otta, who was a manager employed in the City's Technology & Innovation Department ("TID"), Business Information Technology Office, managing the City's email, web and mobile telephone devices. Mr. Otta had administered the Blackberry devices and BBM system, including its 3 day delete feature,

and he assigned the devices to officers selected by the PD. Mr. Otta was aware that the iPhone Office 365 apps and messaging system were not secure and that the PD required a product or app that would mimic or have the security capabilities of the Blackberry devices and BBM.

Mr. Otta had heard of the TigerConnect product, and in late 2013 or early 2014 he arranged for its representatives to meet with and conduct a demonstration of its app with Commander Cox, Lt. Jeffrey Cooper, who was then Acting Administrator, PD IT, as well as civilian PD IT technical professionals Edward Ivora, Tarek Israwi and Doug Lindow.

TigerConnect demonstrated the capabilities of its secure app to replace the Blackberry BBM system, meaning it would be accessible to and serve only those in a controlled group assigned the app, was secure by end-to-end encryption, was not reliant on or connected to the City's servers, had a message self-destruct or message lifespan capability, and provided verification of messages as read. (As with the Blackberry devices, message content archiving was not considered, although TigerConnect can provide that service.¹¹) Because TigerConnect was just beginning to market outside the healthcare industry, it could not provide referrals to the PD to other government or law enforcement agencies familiar with the product.

This review found that the PD decided to acquire the product after a collaborative discussion and review with staff from PD and PD IT, TID, and supervisors, including Commander Cox's supervisor, Deputy Chief David Hendricks, who headed the Investigations Division. In January 2014, the PD began conversations with TigerConnect to purchase the app. (Commander Cox recalls that the PD did not consult then-Chief McDonnell nor then-Deputy Chief Luna, who headed the Patrol Division, on the purchase of TigerConnect.)

The cost of the TigerConnect product was \$11,888, which included \$9,888 for a one-year subscription for 103 licenses (the number of iPhones or devices on which the app could be installed), plus a one-time implementation fee of \$2,000. Commander Cox originated a Technology Services Request for Services Form for the purchase of TigerConnect on May 22, 2014, and it was approved by Lt. Cooper on that date and sent to Mr. Otta, who received the agreement from TigerConnect on May 29. On May 30, Mr. Otta forwarded it to Justina Francisco, an Administrative Analyst in TID, for processing with a copy to Jack Ciulla, Manager, Business Information Systems Bureau, Technology and Innovation Department. Mr. Otta's transmitting email included a message to Mr. Ciulla stating that "[t]his is a product that PD needs for secure texting, something they had on the blackberry [sic] device." The original Purchase Order was approved by Mr. Ciulla on June 5, 2014. Mr. Ciulla approved the TigerConnect invoice for payment on June 11, and payment was made on June 17 by TID. The purchase was not processed through the City's Financial Management Department review chain because it was below the \$25,000 Department purchasing threshold which could be approved by a Commander (or Acting) or higher ranking PD officer. (In later years---2015, 2016, 2017 and 2018, the TigerConnect bill was paid directly by the PD by its own Purchase Orders, as authorized by a Commander or higher level officer.)

There is no evidence that TigerConnect was acquired other than in conformance with the spending approval and technology acquisition policies of the PD and the City.¹²

Deployment of the TigerConnect App

Concurrently with the purchase of TigerConnect, Commander Cox worked with Mr. Israwi on deploying the TigerConnect app. On May 19, 2014, Mr. Israwi sent an email to Vene Sy, who was charged with administering mobile devices for the City's Technology and Innovation Department, and Mr. Otta, with copies to Lt. Cooper, Commander Cox and Mr. Lindow, the latter of whom would be designated as the administrator of the TigerConnect system working in PD IT. The email listed the various apps the PD wanted installed on its iPhones, including TigerConnect (then referred to as TigerText). On May 21, Mr. Israwi created a change Request Ticket in the name of Lt. Cooper and a list of users for the secure TigerConnect app and forwarded that to Ms. Sy via email the following day. Ms. Sy later "pushed" the TigerConnect app to 103 iPhones as assigned by the PD. Users were PD command level and sworn officers in designated units/assignments, a Deputy Chief Administration Bureau Manager and a select Bureau secretary. (In the ensuing time period, with personnel changes, the TigerConnect app was deleted from certain devices and added to others by the administrator, Mr. Lindow, who is a System Support Specialist Supervisor in the Technology and Innovation Department, who also managed the settings for the app.) Since its deployment in 2014, the TigerConnect app has been installed on a total of 145 PD devices, as it was deactivated on some devices and activated on others.

By July or August 2014, the PD had completed the switch to iPhones, including those equipped with TigerConnect.

This review found that there was no discussion of policy within the PD in connection with the deployment and use of TigerConnect because it was viewed as merely a replacement for the Blackberry BBM system previously in use for years.

Use of the TigerConnect App

Based on metadata supplied by TigerConnect, from September 30, 2014, (the earliest date the data is available) until the PD suspended use of the app on September 18, 2018,¹³ PD users of the TigerConnect app logged 261,799 messages to the group's system recipients. (A single message sent by one user to multiple recipients are logged per recipient.)

This review found that TigerConnect provides the PD users with a constant and reliable means of transitory, immediate and secure communication. There is certainty of messages being read because of the system's message prompt.

The TigerConnect messaging app is used for notification within and between members of the assigned group concerning emerging events or incidents, whereabouts, and time and need to respond. (An example of a TigerConnect message chain was provided by Chief Luna, who took a screen shot of a message chain on his device on the

day the app was voluntarily shut down, September 18, 2018. That message chain is attached at Appendix A to this report.)

This review found that TigerConnect is used for “call outs,” operational planning, needs and communication and the status or results of operations in nearly real time. Some messages can be completely inconsequential, such as requesting a “call back” or other contact information. It has proven to be more flexible, efficient, speedy and effective than a telephone call or in person conversation because of its continuous operation, message prompts and ability to message multiple parties in a single use and produce read receipts and string responses. Messages on the app may be dictated by voice to text, increasing its ease and speed of use. Notifications are signaled by an audible tone or a vibration and the app will continue to notify the recipient every two minutes for twenty minutes that a message has been received and is to be read. Messages can be forwarded to other individuals with the app, but not outside that group.

At the October 9, 2018, Public Safety Committee meeting, Deputy Chief Richard Conant addressed the committee. When asked what the PD had done to substitute for TigerConnect since its use was suspended on September 18, 2018, Deputy Chief Conant replied “in the old fashioned way---by telephone calls and in person conversations” and noted that this had degraded the PD’s efficiency and effectiveness in accomplishing its mission.

This review found that the TigerConnect app is not used for “note taking” or as a replacement for any aspect of PD official report writing or evidence retention. Police officers commonly write “notes” by hand, as that is the most efficient process. When necessary, officers transfer information from such notes to official reports. This is a long-standing and common practice in law enforcement. Such notes are then commonly (and lawfully) disposed of. TigerConnect is not a note-taking or data storage app or system.

There is no evidence that the PD’s use of TigerConnect is in violation of City or PD regulations or policies.¹⁴

No Evidence Supports Claims of Illegal Use or Misuse of TigerConnect, No Complaints or Reports of Adverse Effects in Criminal or Civil Cases

There have been no complaints made to the City or to or within the PD regarding any individual’s use, misuse or abuse of the TigerConnect app. This review found no known instances of illegal or misuse of the app.

The Los Angeles County District Attorney’s Office and Long Beach City Prosecutor advise that there have been no issues created in or of any adverse effects on any criminal matters prosecuted by those offices which were investigated by the PD as a result of the use of TigerConnect (or Blackberry before that). Neither office expressed any concerns with the PD use of the technology.

The City Attorney reports there have been no adverse effects in civil cases affecting or involving the City, nor has any litigant or court of record raised a concern over the use of the TigerConnect app by the PD.

Under existing Department policy, PD officers are trained and required to retain exculpatory, as well inculpatory, information and evidence and to report on these matters in writing, and retain evidence, so all this information and matter is available for discovery in criminal and civil litigation.¹⁵ These reports and retained evidence constitute the official record of the PD; TigerConnect instant messages are not, nor have ever been, considered an official record of the PD.

In a September 18, 2018, article, *Al Jazeera* reported that the PD “may have used [TigerConnect] to share sensitive and potentially incriminating¹⁶ information that they wouldn’t want to be disclosed to a court.” The article went on to report that “[two] police officers who spoke with *Al Jazeera*...claimed they were instructed by their superiors to use the app to ‘have conversations with other officers that wouldn’t be discoverable.’ They said they understood this to include exculpatory evidence that could be potentially helpful to attorneys in both civil and criminal proceedings against the department.” The story further reported that the ACLU believes the PD “could be breaking laws that require the preservation of records and the rules that require their disclosure during legal cases, potentially putting thousands of court verdicts at risk,” and a Deputy Public Defender was quoted as saying “his office might now be forced to review all Long Beach cases since 2014, adding: ‘I don’t know what information is in those Tiger Texts, it could be exculpatory, it could lend to practices that are unconstitutional or even illegal.’” “In response to *Al Jazeera*’s investigation, PD said it ‘complies with all laws related to discovery, and any information relevant to a specific investigation would be documented and provided according to legal requirements.’”¹⁷

At the October 9, 2018, Public Safety Committee meeting, Deputy Chief Conant denied there had been any such orders by or within the PD to use TigerConnect to have discussions that would not be discoverable, or to use it as a means to suppress exculpatory information or evidence.

The allegations themselves make no sense nor do they have any inherent logic. TigerConnect is a messaging app. It permits conversations by, between and among the authorized users by means of electronic digital messaging, commonly dictated by voice, as a substitute for telephone conversations or face-to-face conversations. If an officer wanted “to share sensitive and potentially incriminating information” and not have it “disclosed in court,” or to have conversations that wouldn’t be “discoverable,” or to suppress exculpatory evidence in violation of City policy and State and federal law, the officer would hardly be expected to reduce the information into electronic written form (which is itself retained for five days), and transmit it to other officers. The officer would simply conduct any such activity outside of City policy in person via a telephone call or a face-to-face conversation. Neither a telephone call nor face-to-face meeting is available for “disclosure in court” or for “discovery,” unless the participant(s) are subpoenaed to testify to such conversations or meetings. The use of the TigerConnect app to conduct conversations changes none of that because the content and intent of

messages exchanged via TigerConnect can also be testified to if the participants are likewise subpoenaed to testify.

As discussed later in this report, the speculation offered by the ACLU and a Deputy Public Defender that the use of the TigerConnect app by the PD might have violated various laws and court decisions is simply sensational conjecture and, as a matter of law, inaccurate.

If there is or has been a lapse in preserving exculpatory evidence or other information for discovery purposes or disclosure in court, that would lie with failures to adhere to the PD's report writing and evidence retention practices, training and compliance measures. However, there is no evidence of any such lapses and no evidence that the use of the TigerConnect app has contributed to any shortcomings in complying with these policy and legal requirements.

Despite the PD's and City's prompt and well noticed interim suspension of the use of the TigerConnect app the day the article was published, the creation of a website on the issue and widespread announcement by the City and in the media of this independent, outside investigation, no individual, including the two unnamed officers, has come forward to make or substantiate any of the claims reported in the article.

An individual, in a media article he authored, claimed knowledge of or contact with "two separate inside sources,"¹⁸ but he has refused to identify them for purposes of this independent outside review or to offer any evidence to substantiate the claims reported in that article. That same individual appeared at a public meeting of the City's Citizen Police Complaint Commission to register a complaint about the PD's use of the TigerConnect app and to request an investigation, other than the one reported here. This same individual claimed, in an article published in a local newspaper under his byline, that the Los Angeles County District Attorney's Office had confirmed that it "has opened an *investigation* into the Long Beach Police Department's illegal use of the self-deleting message application---TigerText [sic]....."¹⁹

Contrary to this reporter's claims, the Los Angeles County District Attorney's Office is not conducting an "investigation" of the PD's or any individual officer's use of the TigerConnect app. According to the District Attorney's Office Media Relations Division, the complaint was made by the same individual who reported the alleged investigation and that complaint was referred to the District Attorney's Office Justice Integrity Division for "review." The District Attorney's Office media office later responded to this individual specifically and to the wider media, stating that "[i]t is incorrect to characterize our involvement as an investigation."

LEGAL AND POLICY IMPLICATIONS FOR THE USE OF TIGER CONNECT BY THE PD

Compliance with City and Departmental Policies

As noted, when the PD researched, acquired and deployed TigerConnect, there was no effort to address policy issues because the TigerConnect app was viewed as

merely mimicking and replacing the secure, self-destructing features of Blackberry BBM, which had been in use by the same group of officers within the PD for years without any concerns being expressed or problems arising. It was simply viewed as a swap out of one messaging technology platform for another.

The policy implications raised by TigerConnect and the concerns raised in the media and among the public concerning its use by the PD relates to its self-destruct feature which eliminates and makes unrecoverable the content of all messages sent and received using the app. This is essentially an issue of records retention.

This review found that the use of the TigerConnect app, as deployed, is in compliance with existing and emerging policies of the City concerning records retention.

The City is subject to and follows the record retention requirements of state law as set forth in Government Code section 34090, the Guidelines promulgated by the California Secretary of State pursuant to Government Code section 12236, and Section 1.28 of the Long Beach Municipal Code.²⁰ These policies and procedures are all subject to Charter provision Section 2300, which provides: "Notwithstanding any express or implied records retention provisions of this Charter to the contrary, officers and employees of the City are not required to keep, maintain or preserve any City records or writings of any kind or character in excess of the period prescribed by the general law of the State of California."

The City's policy addressing instant messaging, like that conducted via TigerConnect, is Administrative Regulation, AR-8-17, Electronic Mail and Instant Messaging Use and Retention Policy (Revised May 2009). As stated, the purpose of the policy is "to ensure the proper use of the City of Long Beach's Electronic Mail (email) System and Instant Messaging Services."

Electronic Mail Section G provides:

"G. The email system shall be used for transmission, not storage. The City provides *the email system to covered individuals as a convenient and efficient method of rapidly communicating transitory information in an electronic format*. The email system is specifically intended and designed to be a tool for transmission of information, and not a tool for storage of information. Any email that must be retained should be preserved and transferred to an appropriate storage format. Examples of appropriate storage formats include archiving the email, printing a hardcopy, or saving the information as a PDF.

"All users conducting email as a means of communication are individually accountable for determining if the content of an email message, whether sent or received, is subject to their respective department's record retention requirements. In accordance with E-Discovery Law, it is the responsibility of the covered individual to cease destruction of any relevant electronic information concerning any reasonably foreseeable litigation action.

“All relevant electronic information subject to terms of the E-Discovery Law should be preserved and transferred to an appropriate records storage format. Any questions users have with regard to email retention requirements should be brought to the attention of his or her supervisor prior to the disposal of the email.

“Users may archive messages where they can be saved for an indefinite period of time. While the network has adequate capacity for normal City operations, users must be careful in their treatment of items that use an inordinate amount of computer memory, such as graphics, audio and video clips. Delete any such items that are not necessary. Archived email can be saved for an indefinite period of time.

“For file management and storage purposes, most email should be managed within resource capacity. Email concerning City policies, decision-making, proceedings, project or contracts, or that may later be important or useful for carrying out City business operations should be archived, and in the case of a Public Record, saved in an appropriate file. Examples of appropriate storage formats include printing a hardcopy, archiving the email, or saving the information as a PDF.

“When an active email file approaches the threshold size, the system sends a warning message. If the email file size is not reduced and the active file reaches the maximum limit, the system sends another message, no longer allows the saving of Sent email, and may result in delivery failures or delays.

“Users subject to this policy should regularly (once a week) review their mailboxes or folders that contain emails and clean out emails that are not required to be kept by law, this policy, or that are unnecessary for the discharge of official City duties or the conduct of City business, or that are otherwise no longer needed.”

Instant Messaging Sections C., D., and E. provides:

“C. All individuals using IM as a means of communication are individually accountable for determining if the content of an IM message, whether sent or received, is subject to their Department’s record retention requirements. It is the responsibility of the user to retain applicable information.

“D. Information concerning City policies, decision-making, proceedings, project or contracts, or that may later be important or useful for carrying out City business operations should be retained as permanent City records in accordance with City policy. Any information from an IM message required to be retained should be transferred to a records storage system.

“E. Any questions covered individuals have with regard to *applicable transitory retention requirements of a particular IM message or dialogue* should be brought to the attention of his or her supervisor prior to the disposal of the message.”(Emphasis added.)

This policy makes clear that both emails and instant messages are considered by default to be “transitory” and not subject to records retention. Indeed, the email policy explicitly directs users to “clean out” emails regularly. Except as otherwise stated, because the particular content of an email or instant message would require it be retained and transferred to a City archive platform, there are no retention requirements with respect to “transitory messages,” which is the precise nature of messages conveyed on the TigerConnect app.²¹

On April 7, 2017, far in advance of the controversy regarding TigerConnect, the City Attorney and City Manager promulgated to the Mayor and City Council a new Proposed Policy Regarding Use of Private Electronic Devices to Conduct City Related Business. Relevant to this matter is Paragraph 14 of that Policy Proposal:

“Typically, *transitory information that is of a temporary or brief duration, not meant to be kept for future reference and whose value is comparatively short-lived, including, but not limited to, texts, instant messaging, voice mail, or email messages are not the types of documents required to be retained by the City or a City official.* However, transitory communications may be subject to a Public Records Act request if they involve City business, and the City official elects to retain the communication on their City owned or privately owned devices or accounts. If a City official is unsure whether a particular record is a City record for retention purposes, the City official should contact the City's Records Coordinator, his or her immediate supervisor, or the City Attorney's office.” (Emphasis added.)

While full implementation of this policy remains in the meet-and-confer process, the City is generally presently operating within the policy, per the Technology and Innovation Department.

It appears, therefore, that the ephemeral or self-destructing feature of TigerConnect, after 5 days, is consistent with the City's records retention policy, so long as each user retains and transfers to a City archive platform information that is otherwise required to be retained.

This policy regarding “transitory” messages is consistent with state law,²² as state law does not require the retention of “transitory” communications or information because they do not qualify as a “public record” for records retention purposes. The Attorney General has opined that records subject to the records destruction/retention law “constitute[] an objective, lasting indication of a writing, event or other information which is in the custody of a public officer and is kept either (1) because a law requires it to be kept, or (2) because it is necessary or convenient to the discharge of the public

officer's duties, and was made or retained for the purpose of preserving its informational content for future reference.”²³

The evident conclusion to be drawn from this analysis of local agency records retention/destruction by the Attorney General is that City records that are an objective, lasting indication of a writing, event or other information in the custody of a public officer that are required to be kept by law must be kept as required, in accordance with the general retention requirement of 2 years or any applicable requirement prescribing a longer or shorter retention time.²⁴ Records which are not subject to the records retention laws may be destroyed at any time once they have served and are no longer needed for their intended purpose. Clearly, PD users of TigerConnect are aware the messages sent and received on the app will not be retained beyond the 5 day period and intend such. Therefore, City employees are able to create records---emails, as well as instant messages---intended to serve temporary or short term purposes (as long as they are not otherwise required to be retained by law) without becoming obligated to retain them longer term, or to obtain authorization to destroy them.

There is no statute that expressly requires the retention or regulates the destruction of all City emails and instant messages, subject to the nature of their contents, which City policy comprehends. Therefore, the vast majority of emails and instant messages, even those relating to the conduct of the public's business prepared, owned, used or retained by local agencies may be subject to destruction at any time, unless they are made or retained for the purpose of preserving their informational content for future reference, or are subject to special records retention requirements, notably as required by City policy.

Compliance with the Public Records Act (Gov't Code § 6250 *et seq.*)

The Public Records Act (“PRA”) guarantees the right of the people to have access to and inspect “public records.”²⁵ Some open government advocacy entities and individuals object to the destruction, whether manually or automatically, of emails and instant messages created by officials and employees of public agencies in the course of their employment and concerning the conduct of the public's business, claiming such destruction thwarts and runs afoul of the PRA. It does not.

It is true that an email instant message or text message can be considered a “public record” under the PRA.²⁶ Thus, if an email or instant message exists at the time a request for disclosure under the PRA is made and the email or text otherwise satisfies the definition of a “public record” under the statute---“any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any ...local agency”---and comes within the scope of the request, it is subject to disclosure, but may be withheld if an exception to disclosure exists under the law, two of which could apply in such an instance.²⁷ This review found that it is the City's practice to disclose those records unless the record clearly fits one of the exceptions to disclosure set out in the PRA.

However, the PRA is a records disclosure law, not a records retention/destruction law, and its provisions defining a “public record” subject to disclosure under the PRA

does not act to define what constitutes a “public record,” or what some refer to as an “official record,”²⁸ for purposes of records retention/destruction. The definitions in the PRA of “writings” which qualify as “public records” are all expressly limited to the PRA,²⁹ itself, and have no effect on any other provision of law. The general records retention statutes applicable to most City records, including most emails, do not define the records to which they apply. Rather, case law defines records subject to the records retention statutes applicable to the City as “objective, lasting indications of a writing, event or other information which is in the custody of a public officer and kept either because a law requires keeping it, or because it is necessary or convenient to the discharge of the public officer’s duties, and that were made or retained for the purpose of preserving their informational content for future reference.”³⁰

Therefore, the self-destruction of messages on the TigerConnect app, and the policies of the City permitting that function, do not run afoul of the PRA or prevent compliance with that law.

Compliance with Constitutional and Statutory Evidence Retention and Disclosure Obligations in Criminal Prosecutions

*Brady*³¹ is the well-known rule of constitutional criminal procedure which requires the prosecution in all criminal cases to disclose to the defense without request material exculpatory evidence³² which bears on guilt or sentencing. This disclosure obligation is designed to protect a defendant’s 5th and 6th Amendment right to due process of law and a fair trial. If a prosecutor fails to disclose *Brady* matter based upon post-conviction review of the trial and proceedings, any conviction or sentence affected by the failure to disclose is reversed or set aside.³³

An issue in applying the *Brady* disclosure obligation is the question of what evidence the prosecution is responsible or charged with knowing of and disclosing. The *Brady* jurisprudence has created the notion of the “prosecution team.” Under this rule, the prosecutor is responsible for disclosing all material exculpatory evidence known to and in the hands of the “prosecution team,” which includes police agencies involved in the investigation of the charged offenses.³⁴ Therefore, in every criminal prosecution in which the PD is an investigating agency, the prosecutor, whether the City Prosecutor, District Attorney or United States Attorney, is responsible for knowing of---knowledge is automatically imparted or imputed---and disclosing any material exculpatory evidence known to or in the actual or constructive possession of the PD, regardless whether the PD has disclosed the matter to the prosecutor.³⁵

However, as with the distinction between disclosure of “public records” under the PRA and retention/destruction of records under the statutes and jurisprudence regulating those measures, *Brady* imposes a disclosure obligation, albeit a limited one.³⁶ A lesser known constitutional doctrine is one that was recognized in the case of *California v. Trombetta*³⁷ which gave rise to a constitutional due process obligation to preserve certain evidence in the possession of the police or prosecution for the benefit of the defense in a criminal prosecution. Thus, *Trombetta* creates a doctrine more akin to that of records retention/destruction, while *Brady* is a disclosure doctrine closer akin to disclosure under the PRA. Accordingly, the *Trombetta* doctrine is more relevant to the

issue of the propriety of the self-destruction of instant messages sent and received on the TigerConnect app as deployed and used by the PD.

The California Court of Appeal recently explained the differences between *Trombetta*, on the one hand, and *Brady*, on the other, how the *Trombetta* retention obligation is different from the *Brady* disclosure obligation, and ultimately what that retention obligation means.³⁸ That discussion is excerpted here:

“The prosecution's duty to disclose and retain evidence stems from the due process clause of the United States Constitution, as explained and interpreted by the three leading United States Supreme Court decisions on this subject-- *Brady, supra*, 373 U.S. 83, *Trombetta, supra*, 467 U.S. 479, and *Arizona v. Youngblood* (1988) 488 U.S. 51 (*Youngblood*).

“*Brady* is the leading case on the prosecution's duty to disclose exculpatory evidence. ‘[T]he suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material to either guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.’ (*Brady, supra*, 373 U.S. at p. 87.) Such evidence must be disclosed if it is material, that is, if there is a reasonable probability the evidence might have altered the outcome of the trial. (*United States v. Bagley* (1985) 473 U.S. 667, 682.)

“The duty to retain, rather than simply disclose, potentially exculpatory evidence is somewhat different.... ‘Whatever duty the Constitution imposes on the States to preserve evidence, that duty must be limited to evidence that might be expected to play a significant role in the suspect's defense. To meet this standard of constitutional materiality, [citation], evidence must both possess an exculpatory value that was apparent before the evidence was destroyed, and be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means.’ (*Id.* at pp. 488–489, fn. omitted.)

. . . .

“The court [in *Youngblood*] stated: ‘The Due Process Clause of the Fourteenth Amendment, as interpreted in *Brady*, makes the good or bad faith of the State irrelevant when the State fails to disclose to the defendant material exculpatory evidence. But we think the Due Process Clause requires a different result when we deal with the failure of the State to preserve evidentiary material of which no more can be said than that it could have been subjected to tests, the results of which might have exonerated the defendant.’ (*Youngblood, supra*, 488 U.S. at p. 57.) As explained in *Trombetta*, the court noted the problematic nature of determining the materiality of permanently lost evidence. The court also declined to impose on the police an absolute duty to retain and preserve anything that might possibly have some significance. (*Id.* at p. 58.)

“Accordingly, ‘We think that requiring a defendant to show bad faith on the part of the police both limits the extent of the police’s obligation to preserve evidence to reasonable bounds and confines it to that class of cases where the interests of justice most clearly require it, i.e., those cases in which the police themselves by their conduct indicate that the evidence could form a basis for exonerating the defendant. We therefore hold that unless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law.’ (*Youngblood*, *supra*, 488 U.S. at p. 58.) The court held that at worst, the conduct of the police in *Youngblood* could at best be characterized as negligent. (*Ibid.*)

....

“The California Supreme Court has summarized the requirement to retain evidence and when the failure to do so violates due process as follows. The prosecution’s ‘failure to retain evidence violates due process only when that evidence “might be expected to play a significant role in the suspect’s defense,” and has “exculpatory value [that is] apparent before [it is] destroyed.’ [Citation.] In that regard, the mere ‘possibility’ that information in the prosecution’s possession may ultimately prove exculpatory ‘is not enough to satisfy the standard of constitutional materiality.’ [Citation.] And whereas under *Brady*, *supra*, 373 U.S. 83, the good or bad faith of the prosecution is irrelevant when it fails to disclose to the defendant material exculpatory evidence [citation], a different standard applies when the prosecution fails to retain evidence that is potentially useful to the defense. In the latter situation, there is no due process violation unless the accused can show bad faith by the government. [Citation.]” (*City of Los Angeles v. Superior Court* (2002) 29 Cal.4th 1, 8.)”³⁹

Applying these constitutional standards to the intended and actual use of the TigerConnect app by the PD, there is nothing to suggest that its use has or would transgress the duty to retain evidence required by *Trombetta*. The duty to retain evidence under *Trombetta* is “limited to evidence that might be expected to play a significant role in the suspect’s defense, [and] [t]o meet this standard of constitutional materiality, evidence must both possess an exculpatory value *that was apparent before the evidence was destroyed, and be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means.*” (Emphasis added.)⁴⁰

With regard to the instant messages conveyed via the TigerConnect app which are automatically deleted 5 days later, there is nothing to suggest that they would be expected to play a significant role in the suspect’s defense and possess *apparent* exculpatory value to a future prosecution, and more importantly, that such evidence would not be made available to the defense through other “reasonably available means,”⁴¹ namely by inclusion of such evidence in police reports and via evidence

retention procedures.⁴² Again, if there are failures with respect to evidence retention (and ultimate disclosure to the defense) it rests with failures in the report preparation and evidence retention procedure, and not with use of the TigerConnect app which is not a reporting or data or records retention mechanism. Further, the automatic deletion of such messages is proof of an absence of “bad faith” required under the *Youngblood* more demanding standard of “potentially useful” evidence.⁴³

Analogous to the automatic deletion of TigerConnect messages is the common practice in law enforcement of taking raw notes, usually by hand, and then disposing of those notes after relevant information in them are incorporated in a police report. Courts have specifically held that this practice does not violate *Trombetta*.⁴⁴

Finally, it is worthy of note that both the Los Angeles County District Attorney’s Office and the Long Beach City Prosecutor report no *Trombetta* (or *Brady*) or statutory discovery issues have arisen in cases prosecuted by those offices in which the PD was an investigating agency in the years of its use of the Blackberry BBM and TigerConnect app.

Compliance with Civil Litigation Evidence Retention & Discovery Requirements (“spoliation of evidence”)

Matters responded to and/or investigated by the PD, as well as its operations and procedures, can become the subject of civil litigation, most prominently claims based on alleged federal civil rights violations as well as state law based tort claims. There is a duty in the law for a civil *litigant* to preserve what they know or reasonably should know will be relevant evidence in a pending lawsuit or one in the works, even though no discovery request or order to preserve evidence has been made.⁴⁵

Violation of this legal obligation is commonly referred to as “spoliation of evidence.” Spoliation is the willful destruction (or alteration) of evidence, or the failure to preserve matter for another’s use as evidence in pending or reasonably foreseeable litigation.⁴⁶ Spoliation does not itself give rise to a cause of action⁴⁷ or to substantive claims or defenses in civil litigation, but spoliation, if found, may give rise to court imposed sanctions on the offending litigant.⁴⁸

The scope of activity covered by the spoliation rule and the obligation to preserve evidence is limited. Neither the California Civil Discovery Act⁴⁹ nor any California appellate jurisprudence specifically bars the destruction of evidence prior to the filing of a lawsuit. The California courts have suggested that the duty to preserve evidence does not arise until the party is served with discovery demands, even after a lawsuit has been filed.⁵⁰ Moreover, the California Supreme Court has strongly suggested that spoliation claims are meritless where the evidence was destroyed innocently in the ordinary course of business.⁵¹ In the context of electronically stored information (“ESI”), as relevant here, this notion advanced by the court is consistent with the Civil Discovery Act which prohibits the imposition of discovery sanctions when electronically stored information is lost, damaged or overwritten “as a result of the routine, good faith operation of an electronic information system.”⁵²

The operation of the TigerConnect messaging app would not, outside the context of active litigation (in connection with which it should not be employed, and there is no evidence that this has occurred), be considered spoliation subject to any type of discovery sanction by the courts, resulting in prejudice to the City in its litigation.

Federal law might be viewed as extending the scope of spoliation a bit broader to “reasonably foreseeable” litigation.⁵³ However, under even this expansive view of the rule, the good faith, routine use of the TigerConnect app by the PD would not reasonably be expected to run afoul of the federal rule. Indeed, as applied to ESI, which is the relevant consideration here, FRCP Rule 37 (e) Failure to Preserve Electronically Stored Information,⁵⁴ limits sanctions in federal litigation only when “electronically stored information *that should have been preserved in the anticipation or conduct of litigation* is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court: (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or (2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation” may impose terminating sanctions. (Emphasis added.)

Notably, while ephemeral messaging, like TigerConnect, should not be used in connection with the conduct of litigation, itself, and there is no evidence of any such use by the PD, as late as September 2018, and, no court has imposed sanctions as a result of ephemeral communications related spoliation, according to reliable reporting.⁵⁵

The City Attorney reports that the use of TigerConnect by the PD has not had any effect in the civil litigation handled by that office.

“BEST PRACTICES” FOR THE USE OF TIGER CONNECT OR OTHER EPHEMERAL MESSAGING APPS BY THE PD AND THE CITY

Technology inevitably outpaces law and policy. Almost deliberately so. Writing in 2010 for the Court in a case involving the search of text messages on an employee’s city-issued pager, Justice Kennedy noted:

“The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. See, e.g., *Olmstead v. United States*, 277 U. S. 438 (1928), overruled by *Katz v. United States*, 389 U. S. 347, 353 (1967).”⁵⁶

The citation to the *Olmstead* decision serves as a reminder than 80 years earlier the Supreme Court struggled and essentially failed to spell out privacy expectations with respect to the telephone, which by then had been in common use for nearly 20 years. Only 40 years later did the Court decide that there was a right of privacy in a telephone conversation in the *Katz* decision, and the Court had to revolutionize our understanding of the 4th Amendment’s protection of privacy in order to do so.

Cellphones achieved popularity and widespread use by the mid-90's. Within a short period of time more than 90% of American adults owned a cell phone.⁵⁷ The iPhone was introduced in 2007. Yet, it took until 2012 for the Supreme Court to rule on the use of cellphone based GPS surveillance by police,⁵⁸ 2014 to rule on the search of cellphones incident to arrest,⁵⁹ and 2018 to rule on cellphone tower location tracking.⁶⁰ Only in 2017 did the California Supreme Court decide that emails, texts and instant messages on private devices concerning public business are subject to the Public Records Act.⁶¹ Courts and policy makers are understandably hard pressed to keep up with the constant leaps in technology.⁶²

With respect to the PD's use of the TigerConnect app, it did not come to the attention of either the PD's policy-makers---the City Council or City Manager---or the PD's legal advisor---the City Attorney---because the PD and City technology professionals who researched, planned, purchased, and deployed the app believed in good faith that it was merely replacing the same technology in use for years via the Blackberry BBM system, and it was deployed in the same fashion. These professionals followed applicable City purchasing and technology implementation policies, practices and procedures. The TigerConnect app was then in use for over four years without "notice" or incident, either internally or in relation to any civil or criminal litigation related to the PD's operations. There is little doubt that this technology provides a communication tool that offers faster, more reliable communication.

That said, in hindsight, this review finds that the deployment and use of the TigerConnect app by the PD has been consistent with both requirements of the law and applicable City policies, as discussed in this report. Moreover, aside from unsubstantiated claims and speculation, there is no evidence that the PD has illegally used or misused the TigerConnect app in any way.

The media coverage and consequent voluntary suspension of the use of the TigerConnect app by the PD now gives City policy-makers and legal advisors the opportunity to review the technology and its use in an open and transparent manner, and determine whether it is something the City wishes to continue deploying. Additionally, this pause and review provides the space to examine existing policies and make appropriate adjustments or amendments. With this in mind, certain "best practices" are discussed here.

While the abstract possibility of misuse or abuse is inherent with the use of any technology in any human institution, that risk has to be balanced against the utility and efficiencies the technology brings to the enterprise. The actions of every individual are out of the City's control, but its standards can still be refined to promote and enhance both accountability and proper practices.

Here, the PD command and special units have relied for years on secure, encrypted, self-destructing instant messaging technology, where it serves essentially as a superior means of communication over a telephone call or in person conversation. The widespread use of ephemeral messaging in society at large serves to make its use by the PD less exotic and frankly less "questionable," making apprehension around its use

naïve. Such technology is nothing new, and much of the risk it poses can be vastly limited by how it is used and by whom.

One industry expert, Andy Wilson, CEO of e-discovery company Logikcull, has explained that any risk with Gmail's new ephemeral messaging updates is "totally dependent on how these businesses enable and police these types of features and functionality." Confidential model, for example, can be managed at a high level for those using the corporate Gmail applications. "It's an IT administrative feature" for enterprises, Wilson noted. "The users themselves cannot turn it on" without first being allowed to by a manager with administrative Gmail privileges. It is also likely that many companies will have a relatively easy time managing such ephemeral messaging functions given that many have used them in the past. "It's not just Gmail. This technology is not new. There are plugins that have existed for years that allow you to do all the same stuff," Wilson said. Michael Powell, solutions analyst at ZL Technologies, noted that such tools have been commonly used for years by large corporations, government officials and financial institutions like banks to manage sensitive or confidential information and trade secrets.⁶³

The TigerConnect app is deployed to only 103 command level and special unit sworn officers in the PD. These are officers tasked with mission critical management, public safety and law enforcement functions and responsibilities to whom the City places its highest trust. They are expected to meet the challenges of the department's mission and conduct themselves professionally with the assumption that they are there "to do the right thing." The PD has demonstrated the need for and efficiencies resulting from this technology and have employed it for years without incident. On the practical side, the system, itself, is managed by a City technology professional who acts to limit who uses the system and its settings. This is not to say that deployment and use of the TigerConnect app should not be scrutinized, vetted and reviewed by policy-makers, oversight authorities and legal advisors.

The City could now undertake applicable policy review to ensure those measures comprehend this technology, address its uses and are consistent with overall communication policies. The valid operational reasons for using the technology should be spelled out and be set forth clearly, in addition to the procedures controlling its use. This will act to ensure compliance with legal requirements and policy preferences going forward, avoid misuse or abuse, and put the use of the technology on sound and transparent footing. Thus, it is recommended that the Police Department and the City undertake the following measures to ensure "best practices" are implemented and followed:

- The Police Department should create a specific policy related to TigerConnect or other similar messaging applications to clearly outline the valid operational reasons for using the technology and the procedures for controlling its use. Any policy should clearly outline, as other City policies currently do, the responsibility of the user to preserve any records that fall under the records retention policy in a different system than the Instant Messaging System

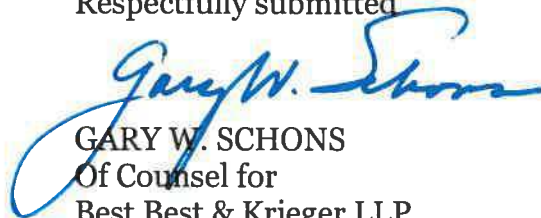
- The City should initiate the meet-and-confer process for any new policy or change in policy resulting from this review
- The City should continue to ensure that any system is centrally managed by an individual responsible for overall system management, to control authorized users and global settings such as length of time to retain a message
- The current 5-day message expiration should be reviewed to determine whether the City wishes to keep or extend this time. The City should also review whether the archiving function should be utilized. It is a policy decision of the City to determine the appropriate amount of time to retain messages and whether to archive them
- The Police Department should conduct a review of the currently authorized users and establish formal procedures for adding or removing individuals based on their job assignment that requires access to the TigerConnect system
- The city should finalize the meet-and-confer process and implement the City's Proposed Policy Regarding Use of Private Electronic Devices to Conduct City Related Business and distribute to all City staff

David Feldis, a partner at the law firm of Perkins Cole LLP, noted, "In 2018, it is likely not a satisfactory answer for a company to say it has not considered or anticipated the use of the many types of dynamic, encrypted or disappearing communication applications that are now prevalent."⁶⁴

Following a thoughtful review and policy creation process, should the City elect to permit the PD to reinitiate the use of the TigerConnect app, it will then be able explain to its residents and other stakeholders the reason for the use of this ephemeral messaging app by the PD, and perhaps other City departments, and dispel the suspicions and accusations which prompted this review.

Dated: November 30, 2018

Respectfully submitted



GARY W. SCHONS
Of Counsel for
Best Best & Krieger LLP

END NOTES

¹ <http://www.longbeach.gov/globalassets/police/media-library/documents/how-do-i/tiger-connect/9-18-19-special-order-tiger-connect>

² <http://longbeach.gov/police/how-do-i/public-records-requests/tiger-connect-communication-application/>

³ <http://longbeach.gov/press-releases/city-of-long-beach-initiates-outside-review-of-police-department-direct-messaging-application/>

⁴ See, n. 3, *supra*.

⁵ TigerConnect is the name of the company which produces this messaging app. When the product was first purchased by the Long Beach Police Department in 2014, it was known as TigerTextPro. It is now known as TigerTextEssentials. In this report, this secure messaging app will be referred to as TigerConnect, as will the company. TigerConnect offers an unsecure downloadable messaging app known simply as TigerText. That product is not relevant to or discussed in this report.

⁶ “Instant messaging” and “text” or “texting” are used interchangeably in this report, and given their common sense, non-technical meanings.

⁷ Schnitzler, Utz, Farke, Popper & Durmuth, *User Perception and Expectations on Deleting Instant Messages —or— “What Happens If I Press This Button?”* (2018) European Workshop on Usable Security https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurosec2018_09_Schnitzler_paper.pdf

⁸ Wickr offers fully encrypted enterprise-level communications that are automatically deleted after a specified period of time.

⁹ <https://www.law.com/legaltechnews/2018/06/22/is-gmails-new-ephemeral-messaging-service-a-threat-to-data-retention/>

¹⁰ Doug Austin, Vice President, Cloudnine, speaking at Relativity Fest, October 2018 on “Social Media Law and Practice.”

https://rfi18.smarteventcloud.com/connect/sessionDetail.wv?SESSION_ID=227576&tc=popup

¹¹ TigerConnect archiving would cost the City \$960 annually.

¹² See, Administrative Regulation, No. AR-8-23, Use and Procurement of City Telephones and Service.

¹³ The City’s September 18 statement on Chief’s order suspending use of TigerConnect provided: “Effective immediately, and after consultation with the Offices of the City Manager and City Attorney, and the Chief of Police, the City is suspending any use of the Tiger Connect application pending further review of whether the use is consistent with the City’s record retention policy and administrative regulations for the use of mobile devices. The City has confirmed that no other department, besides the Long Beach Police Department, utilizes Tiger Connect on City mobile devices for public business.

Recent Public Records Act requests and media inquiries prompted the City of Long Beach to initiate a review of its use of the Tiger Connect secure texting communication application. The Tiger Connect application has been used by the Police Department since 2014.

Use of the application began when the Police Department transitioned to iPhones, which did not have a built in secure communication feature sufficient for the needs of the Department. The primary purpose of the Tiger Connect application was to allow for a continued means of transitory, immediate, and secure communications regarding operational and personnel matters. Police Department employees have been trained to and do document any exculpatory/discoverable evidence in a police report or other formal departmental communication.

Of the 291 Police Department-issued mobile devices, the Tiger Connect texting application is installed on 145 mobile devices, including the mobile devices of Command Staff, and specialized details such as Homicide and Internal Affairs. For reference, the Police Department has a total of 1,214 employees.”

¹⁴ See, Administrative Regulation, AR-8-30, Use of City Computers and Related Equipment and Use of Email and Internet Personnel Policies and Procedures, City Computer, Email and Internet Use, No. 1-11, May 20, 2009. Manual of the Long Beach Police Department, § 3.36, Telephones.

¹⁵ See, Long Beach Police Department Training Bulletin, 13-Report Writing, Revised May 2001.

¹⁶ What is meant by “incriminating” in this context is not clear nor is it explained in the article.

¹⁷ <https://www.aljazeera.com/news/2018/09/exclusive-police-tiger-text-app-conceal-evidence-180918052839766.html>

¹⁸ It is not known if these “sources” are the same two officers who spoke with *Al Jazeera* for its article.

¹⁹ <https://beachcomber.news/content/tigertext-review-investigation-or-cover>

²⁰ Long Beach Municipal Code §1.28.010: “Records survive transition of officials. All documents prepared, received or maintained by the office of the Mayor, City Councilmembers, by any elected City official, and by the head of any City Department, are the property of the City. The originals of these documents shall be maintained consistent with State law and the records retention policies of the City as set forth in the City Charter, and by administrative regulation. (See, e.g., City Council Resolution 18-0141, September 18, 2018.) City Administrative Regulation AR-6-1 addresses Records Management.

²¹ An inquiry to City TID sought data on the transfer of emails and instant messages by users to City archive platforms. TID was unable to determine whether and how often this was done with respect to either emails or instant messages and whether it has ever occurred with respect to TigerConnect instant messages.

²² The Records Management Act (Gov. Code 14740-14774) creating the State Administrative Manual and California Acquisition Manual do not apply to local public agencies. “Since, with the exception of the PRA, legislation and directives establishing the state Records Management Program do not apply to local government, county and/or city government agencies do not have a standardized program of accountability for their treatment of public records. Nor does local government have standard retention periods for various record categories other than certain record types identified in government codes that mandate specific local programs. To alleviate this situation the 1999 legislature added Section 12236 to the Government Code, which states in Section 12236 (a) “The Secretary of State shall establish the Local Government Records Program to be administered by the State Archives to establish guidelines for local government retention and to provide archival support to local agencies in this state.” These guidelines are an initial attempt to provide some standards and structure to the local government records management effort. Other attempts at standardization include the California City Clerks Association’s 1998 list of common local government records and recommended retention periods. The goal of the State Archives in compliance with GC 12236 is to consolidate information resources and provide local government with a single source for archival and records management support and guidance. “Definitions: “Retention Period – The length of time a record must be retained to fulfill its administrative, fiscal and/or legal function. Then a record should be disposed of as soon as possible in accordance with an approved Records Retention Schedule.

“Retention Schedules 2-2040

A properly prepared and approved Records Retention Schedule is an agency’s legal authority to do whatever needs to be done with records and documents entrusted to the agency’s care.”

(Secretary of state, Local Government Records Management Guidelines. February 2006.)
<https://archives.cdn.sos.ca.gov/local-gov-program/pdf/records-management-8.pdf>

²³ Attorney General Opinion No. 80-1006, 64 Ops.Cal.Atty.Gen. 317, 326 (1980).

²⁴ The 2 year retention requirement is found in Government Code section 34090, sub. (d).

²⁵ See, Gov’t Code § 6250, “access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in the state.” This statutory provision enacted in 1968 was later underscored by enactment of Senate Constitutional Amendment 1 (2004) which placed nearly identical language in Article 1, Section 3, subdivision (b)(1) of the State Constitution.

²⁶ See, Gov’t Code § 6252, subd. (g) defining a “writing” as, among others, “transmitting by electronic mail.” The California Supreme Court said as much in its decision in *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608, 617 (among the records sought in that matter were emails and text messages on the private devices of city officials).

²⁷ With respect to the instant messages transmitted on the TigerConnect app, if they were available at the time of a request under the PRA and otherwise met the definition of a “public record” owing to their content, they likely would be exempt from disclosure under either the “preliminary drafts, notes or interagency or intra-agency memoranda” exception which applies to memoranda “not retained by the public agency in the ordinary course of business.” (Gov’t Code § 6254, sub. (a).) Alternatively, these messages could be exempt from disclosure under the law enforcement “investigative file” exception contained in Government Code section 6254, subdivision (f).

²⁸ See, e.g., County of Orange, County Records Management Policy, Sept. 26, 2017, “Official records are subject to retention under records retention laws or regulations and/or County records retention policy and/or schedules” distinguishing them from “public records” under the PRA.

²⁹ Gov't Code § 6252 is the definitional section and provides that its definitions apply (only) "[a]s used in this chapter," namely, the PRA, itself.

³⁰ See, Attorney General Opinion No. 80-1006, 64 Ops.Cal.Atty.Gen. at p. 326, *supra*, citing *People v. Tomalty* (1910) 14 Cal.App.2d 9, cited with approval in *Loder v. Municipal Court* (1976) 17 Cal.3d 859, 863-864; *People v. Shaw* (1941) 17 Cal.2d 788, 811; and, *People v. Pearson* (1952) 111 Cal.App.2d 9, 18. See also, *People v. Olson* (1965) 232 Cal.App.2d 480, 486 ("The mere fact that a writing is in the possession of a public officer or a public agency does not make it a public record.")

³¹ *Brady v. Maryland* (1963) 373 U.S. 83, 87.

³² See, *United States v. Agurs* (1976) 427 U.S. 97, 103-104 (the defense need not request *Brady* evidence; the obligation to disclose is self-executing on the prosecution). "Material exculpatory evidence" is defined as evidence for which there is a reasonable probability its admission or use would have altered the outcome of the trial, not necessarily result in an acquittal, but conviction of a lesser conviction or sentence. (*United States. Bagley* (1985) 473 U.S. 667, 682.) One of the difficulties of applying the *Brady* rule, particularly in the abstract, is determining what qualifies as "material" is highly dependent on the evidence introduced in the case and the test can be applied only after a case is tried. (See, *Kyles v. Whitley* (1995) 514 U.S. 419, 439 (Commenting on this conundrum, Justice Souter, writing for the Court, observed: "This means, naturally, that a prosecutor anxious about tacking too close to the wind will disclose a favorable piece of evidence. See *Agurs*, 427 U.S., at 108 ('[T]he prudent prosecutor will resolve doubtful questions in favor of disclosure'). This is as it should be.") This disclosure obligation is carried forth by provisions of the state's Criminal Discovery Act (Penal Code § 1054, *et seq.*), as well as the ethical obligations imposed on prosecutors as attorneys pursuant to the California Rules of Professional Conduct (Rule 3.8 (d), Comment[3]).

³³ See, *United States v. Agurs* (1976) 427 U.S. 97, 103-104.

³⁴ See, *Kyles*, *supra*, 514 U.S. at pp. 437-40. The prosecutorial team comprises all those acting "on the government's behalf," including the police agency that investigated the crime. (*Id.* at p. 437.) Knowledge of evidence favorable to the defense held by members of the prosecutorial team is automatically imparted on the prosecutor who is liable for the disclosure of all exculpatory information or evidence that any member of the prosecutorial "team actually or constructively possesses." (*In re Steele*, 32 Cal. 4th 682, 697 (2004) (quoting *People v. Superior Court*, 80 Cal. App. 4th 1305, 1315 (2000)), see also *In re Brown* (1998) 17 Cal.4th 873, 879.)

³⁵ See, note xxvii, *supra*.

³⁶ Contrary to some assertions about *Brady* and its progeny, the doctrine does not create a constitutional discovery doctrine. (See, *United States v. Ruiz* (2002) 536 U.S. 622, 629, citing *Weatherford v. Bursey* (1977) 429 U.S. 545, 559).

³⁷ *California v. Trombetta* (1984) 467 U.S. 479.

³⁸ *People v. Alvarez* (2014) 229 Cal.App.4th 761.

³⁹ *Alvarez*, *supra*, at pp. 771-773

⁴⁰ *Trombetta*, *supra*, at pp. 488-489.

⁴¹ "Comparable evidence" does not mean *identical* evidence. (See, e.g., *People v. Walker* (1988) 47 Cal.3d 605, 638 (finding the ability to cross-examine officer who monitored defendant's conversation with police was sufficient to overcome the loss of the tape recording of that conversation).

⁴² "A due process violation occurs when the state is aware that the evidence could form the basis for exonerating the defendant and fails to preserve it as part of a conscious effort to circumvent its constitutional discovery obligation." (*Trombetta*, *supra*, 467 U.S. at p. 488.)

⁴³ The absence of "bad faith" in this context means "the absence of malice and absence of design to seek an unconscionable advantage over the defendant." (*People v. Angeles* (1985) 172 Cal.App.3d 1203, 1214.)

⁴⁴ See, *People v. Cole* (2006) 134 Cal.App.4th 10491054-55; *People v. Garcia* (200) 84 Cal.app.4th 316, 331; *People v. Garcia* (1986) 183 Cal.App.3d 335, 347-350.)

⁴⁵ Schwarzer, Tashima & Wagstaffe, Rutter Group Prac. Guide: *Federal Civ. Pro. Before Trial* (Rutter Group-June 2016 Update) Ch. 11 (I)-C, ¶ 11:25.

⁴⁶ See, *United States v. Kitsap Physicians Svs.* (9th Cir. 2002) 314 F.3d 995.

⁴⁷ See, *Cedars-Sinai Medical Center v. Superior Court* (1998) 18 Cal.4th 1, 8-13 (finding other mechanisms, particularly under the Civil Discovery Act to be potent deterrents and remedies.); accord *Williams v. Russ* (2008) 167 Cal.App. 4th 1215, 1223.

⁴⁸ See, *Leon v. IDX sys. Corp.* (9th Cir. 2006) 464 F.3d 951, 958. A party seeking sanctions for spoliation of evidence has the burden of establishing the following elements by a preponderance of the evidence: “(1) the party having control over the evidence had an obligation to preserve it when it was destroyed or altered; (2) the destruction or loss was accompanied by a ‘culpable state of mind;’ and (3) the evidence that was destroyed or altered was ‘relevant’ to the claims or defenses of the party that sought the discovery of the spoliated evidence.” (*Conan v. City of Fontana* (C.D.Cal. 2017 EDCV 16-1261-KK) 2017 WL 3530350.

⁴⁹ CCP § 2016.010 *et seq.*

⁵⁰ See, *New Albertsons Inc. v. Superior Court* (2008) 168 Cal.app.4th 1403, 1430-31. This limit on the scope of the spoliation rule might well apply even to the intentional destruction of evidence relevant to avoid uncertain, inchoate, but possible, liability claims. (See, *Willard v. Caterpillar, Inc.* (1995) 40 Cal.App.4th 892, 907.)

⁵¹ *Cedars-Sinai, supra*, 18 Cal.4th at pp. 15–16.

⁵² CCP § 2023.030 (f)(1).

⁵³ See, *United States v. Kitsap Physicians Svs., supra*; *Zabulake v. UBS Warburg LLC* (S.D.N.Y. 2003) 220 F.R.D. 212, 218.

⁵⁴ Rule 37(e) does not depart from the common law duty to preserve relevant information, but rather authorizes specific sanctions the federal courts may impose.

⁵⁵ See, *When Electronic Records Disappear But Legal Issues Linger*, Fisher, Hamilton & Southwick, September 6, 2018. Law 360 <https://www.law360.com/articles/1077918/when-electronic-records-disappear-but-legal-issues-linger>

⁵⁶ *Ontario v. Quon* (2010) 560 U.S. 746, 760.

⁵⁷ *Riley v. California* (2014) 573 U.S. ____ (Justice Roberts’ majority opinion).

⁵⁸ *United States v. Jones* (2012) 565 U.S. 400.

⁵⁹ *Riley v. California, supra*, 573 U.S. ____.

⁶⁰ *Carpenter v. United States* (2018) 585 U.S. ____.

⁶¹ *City of San Jose v. Superior Court, supra*, 2 Cal.5th 608.

⁶² “Moore’s law” predicts a doubling of the capabilities of digital technology every 2 years.

⁶³ Dipshan, “Is Gmail’s New Ephemeral Messaging Service a Threat to Data Retention,” Legaltechnews (June 22, 2018) <https://www.law.com/legaltechnews/2018/06/22/is-gmails-new-ephemeral-messaging-service-a-threat-to-data-retention/>

⁶⁴ Graham, “WhatsApp, Wickr Seen By Justice Dept. as Tools to Erase Evidence,” Bloomberg Law (May 15, 2018) <https://biglawbusiness.com/whatsapp-wickr-seen-by-justice-dept-as-tools-to-erase-evidence/>

APPENDIX A



Lewis, Michael

Gentlemen, I stopped by the in custody death scene on my way into work. Lab still processing scene. The suspect is actually 51 years old and not late twenties as told last night. Drugs, drug paraphernalia and rehab program literature in house. Info about the suspect and the location being put together. Let me know if anyone needs me to call them.

8:01 AM • 3 days left



Lewis, Michael

Still no media inquiries. I verbally notified Pat West, Modica and Suzie Price.

8:02 AM - 3 days left

Thanks

8:03 AM - 3 days left

5/5 Read



Conant, Richard - Deputy Chief

Thanks Mike. Not necessary, I'm handing the invest side. Appreciate last nights notifications. Rich

8:04 AM - 3 days left

will come from IB.
That's appropriate. But
I appreciate your help.

8:09 AM - 3 days left



Lewis, Michael

Got it..

8:10 AM - 3 days left



Berkenkamp, Jeffrey - Commander

**Rich, can you confirm
if all 5 officers involved
will be off until the
CID?**

9:05 AM - 3 days left



Conant, Richard - Deputy Chief

**Just got in the office.
Will advise.**

9:09 AM - 3 days left

Chief, FYI. the bike shooting incident from last night where the victim was shot in the face. this incident is hispanic vs. hispanic with a known suspect. rich

2:46 PM • 3 days left

Copy, thank you

2:49 PM • 3 days left

Read

Avail for a call

4:22 PM • 3 days left

Yes

4:45 PM • 3 days left

Read

THIS PAGE INTENTIONALLY LEFT BLANK